REMARKS

Claims 1-16 stand rejected under 35 U.S.C. ∋103 as being unpatentable over United States Patent No. 6,253,193 to Ginter et al. in view of United States Patent No. 5,832,083 to Iwayama et al.

Applicants once again respectfully submit that all of the features of independent Claims 1 and 7-15 are not disclosed in the cited references. Specifically, both the Ginter et al. reference and the Iwayama et al. reference fail to disclose or suggest the decoding of license information using the ID information of a plurality of physical elements in which "the license information is partially decoded by a first one of said physical elements," and "then said partially decoded license information is sent to another of said physical elements to be decoded," as defined in the independent claims.

As described on page 10 (line 21) through page 11 (line 3) of the present Specification, one problem to be resolved by the present invention is to prevent illegitimacy overlooked in the case where the license is produced from the usage environment specifying physical element, where the usage environment specifying physical element is simply a large sized device, and part of the device is illegitimate. The present invention prevents such illegitimacy by decoding the license partially by each of the physical elements, wherein the partially decoded license information is moved from one physical device to at least one other physical device for the decoding to be completed.

13

In his response on page 2 (lines 1-9) of the Final Office Action, the Examiner argues that the Ginter et al. reference teaches that multiple pieces of independently managed VDE content can be combined into a single VDE container object; that the combination of VDE managed pieces will frequently require securely deriving content control requirements (including combination rules); and that "Figures I-J [which Applicants believe refer to Figures 11I-11J] teaches about "component" assembly that controls access to data."

Applicants agree with the Examiner's assertions listed in the previous paragraph. However, the teachings mentioned above still lack any disclosure or suggestion that the encrypted license information should be partially decoded within one of the physical elements, and then the partially decoded license information is sent to another physical element to complete the decoding. Initially, in the discussion of component assemblies in columns 79-87, the Ginter et al. reference does not mention decoding the component assemblies. Instead, the discussion of decoding (decrypting) the encrypted information is found in column 67, *inter alia*. Column 67 of Ginter et al. refers to decrypting information using a special purpose encrypt/decrypt hardware engine 522 (shown in Figure 9 within hardware tamper resistant barrier 502, which is also shown in Figure 10). Thus, the complete decoding (decrypting) appears to take place within a single component (hardware engine 522). There is no disclosure or suggestion that the decoding (decrypting) should take place within two (or more) different physical components, as in the present invention. Further, there is no disclosure or suggestion that the decoding should *partially* take place within one

physical component, and that the partially decoded license information should be moved to a second physical component for completing the decoding of the license information.

With regard to the component assemblies shown in Figures 11I and 11J of the Ginter et al. reference, even assuming *arguendo* that each of the various separate components and/or the various component sub-assemblies that make up the component assembly include license information that is to be decoded, there is no disclosure or suggestion that even a single piece of license information is to be partially decoded in one physical element, and then that partially decoded license information is to be moved to a different physical element to complete the decoding. Instead, Figures 11I and 11J appear to simply show that as long as the component assembly has been assembled in an authorized manner, it can be loaded and the components can be used.

The Examiner further argues that layering security techniques is not novel, and that mere duplication of a working part involves only routine skill in the art. Although the Examiner has correctly stated that case law on this issue, Applicants respectfully submit that the claimed invention is more than either the mere layering of known security techniques or the mere duplication of a working part. The present invention does not relate to merely duplicating the concept of decoding encrypted license information by requiring that multiple licenses be decoded by multiple physical elements. Instead, as mentioned earlier, the license information is partially decoded by one physical element, and the partially decoded license information is passed to another physical element for the decoding to be completed. In this

15

manner, the license information is not fully decoded unless all physical elements have authorization. In the case where multiple licenses are decoded by multiple physical elements, certain licenses can be fully decoded (and perhaps used elsewhere), eventhough there are unauthorized physical elements within the system.

Finally, the Examiner analogized the present invention to a situation of requiring opening of multiple doors with multiple separate keys. However, Applicants respectfully submit that the analogy is not accurate. A more accurate analogy would be having a single key and at least two doors, where the key is placed within the first door, and the key is somewhat modified by the first door before placing the modified key into the second door, where, if the modified key is authorized for the second door, it then opens both doors.

More specifically, one example of an embodiment of the present invention that includes this feature is shown in Applicants' Figure 14, which is described on page 41 of the present application. In this embodiment of the license decoding process, the encrypted license includes, among other things, the ID's of the following physical elements --the storage device (device serial number 141), the medium (medium serial number 143), and the reproduction device (ID of reproduction device 144).

Briefly, when the correct conditions are present, the encrypted license information is partially decoded by the storage device 140, and the partially decoded license is sent to the reproduction device 144, which in turn completes the process of decoding the

license. More specifically, in this embodiment, the license generated by the license server 40 has been encrypted by encrypting the access control list (ACL) and the content decode key (Kc) using the key Kp, which is the physical element ID of the reproduction device 144. The license has been further encrypted by using, as a key, the value of the exclusive OR of the DSN 141 and the MSN 143. During decoding, the storage device 140 first reads the MSN 143, and the exclusive OR is calculated between it and DSN 141, whereby the license is partially decoded into {ACL, Kc}Kp. The partially decoded license is then sent to the reproduction device 144, which completes the decoding process of the partially decoded license using the key Kp, which is comprised of the physical element ID of the reproduction device 144. If the access conditions have been satisfied, the content decode key Kc can then be used to decode the content, and the decoded content can be reproduced by the reproduction device.

In contrast, in the device of Ginter et al., license information does not appear to be partially decoded by a first physical device, nor does any partially decoded information appear to be passed through to a second physical device for final decoding and use. Instead, full decoding appears to take place by referencing each physical device separately, without passing license information through one physical device to a second physical device.

To remedy this deficiency, the Examiner has relied upon the Iwayama et al. reference. However, the Iwayama et al. reference also fails to disclose or suggest a device in which license information is partially decoded by a first physical device, and where the

17

partially decoded information is then sent to a second physical device for final decoding and use. As described in column 9 (line 37) through column 10 (line 37) of the Iwayama et al. reference, while making reference to Figure 1, all of the decoding in this device appears to occur within a single physical element (the information transforming (converting) section 1), and there is no disclosure or suggestion of partially decoding license information, nor of sending partially decoded license information to another physical device.

More specifically, in the system of the Iwayama et al. reference, the information transforming (converting) section 1 retrieves encoded data content and encoded content ID information from the data storing section 3. Then, the information transforming (converting) section 1 receives encoded utilization permission information from the utilization permitting device 2, and the information transforming (converting) section 1 decodes the encoded utilization permission information to generate a decoding key. The information transforming (converting) section 1 uses that decoding key to decode the encoded data content and the encoded content ID information. The decoded content ID information is compared against the content ID information input by the user, and if they coincide, the decoded data content is output to the user. Although the Examiner is correct in asserting that the Iwayama et al. reference teaches a plurality of physical elements, in the Inayama et al. reference, all decoding takes place within a single one of those physical elements. Thus, the Iwayama et al. device fails to disclose or suggest partial decoding of license information, where a portion of the decoding takes place in one physical element and

18

that partially decoded license information is sent to another physical element for additional decoding.

In addition, Applicants have also amended independent Claims 1, 7-11 and 15 (but have not amended independent Claims 12, 13 and 14) to recite that the license information is encrypted "in a multiplex way in a predetermined order" and that the license information is decoded "in inverse to said predetermined order." Support for these features can be found in the original specification on page 34, lines 5-10. Applicants respectfully submit that neither the Ginter et al. reference nor the Iwayama et al. reference disclose or suggest these features.

Accordingly, as all of the features of independent Claims 1 and 7-15 are not disclosed in the Ginter et al. reference and/or in the Iwayama et al. reference, Applicants respectfully request the withdrawal of this §103 rejection of independent Claims 1 and 7-15 and associated dependent Claims 2-6.

For all of the above reasons, Applicants request reconsideration and allowance of the claimed invention. The Examiner is invited to contact the undersigned attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

James K. Folker
Registration No. 37,538

August 31, 2004
Suite 2500
300 South Wacker Drive
Chicago, Illinois 60606
(312) 360-0080
Customer No. 24978